THE CITY OF NEWTON

TELECOMMUNICATIONS SYSTEMS USE POLICY

I. INTRODUCTION

The City of Newton's Telecommunications Systems are a finite resource and, as such, the City of Newton has set forth the following guidelines and limitations on authorized and appropriate use, as well as to prevent misuse and illegal use, of its telecommunications systems. This policy will be reviewed periodically and may be updated or amended at any time at the discretion of the Mayor.

II. DEFINITIONS

Telecommunications Systems

Telecommunications Systems - The term "telecommunications systems" refers to any analog or digital electronic device or system that uses, manages, carries, streams, or supports audio and/or video and/or data in any form. This term includes data transmitted or received via telephone, radio, television, cable, wireless, computer systems or fax machines. This term also includes all computer devices connected to a network and to the networks themselves. The definition also includes the hardware and software associated with these devices and systems and all information managed by these systems. For additional terms, please see **Appendix A.**

III. SCOPE OF APPLICABILITY

This policy applies to all users of the City's telecommunications systems. Users include employees, elected or appointed officials and anyone else granted authorized access to the City's telecommunications systems.

IV. POLICY STATEMENT

All users of the City's telecommunications systems must read and comply with this policy. Use of the City's telecommunications systems indicates the user's agreement to be bound by the terms of this policy. Violation of any prohibited use prescribed within this policy or failure to comply with the provisions of this policy may result in disciplinary action ranging from limiting an employee's privileges for access to the telecommunications systems to further disciplinary action, up to and including termination from employment. The appropriate state and federal and local law enforcement agencies may be notified for any use believed to be illegal.

The City's telecommunications systems are the property of the City of Newton, and their use is intended for City business and operations. Any other use may be considered inappropriate use of the City's telecommunications systems.

All network broadcast messages made with or through the City's telecommunications systems must be pre-approved by the Mayor or the Chief Administrative Officer. Only members of the Executive Department or the Department of Information Technology may transmit these broadcast messages.

All users must undertake precautions to prevent infection of any part of the City's computer network by computer viruses. Users are prohibited from downloading computer programs unless they have been authorized by the Department of Information Technology (IT) and they have been subjected to virus detection procedures approved by IT. IT may, from time to time, impose additional restrictions or regulations on the importing of remote files, and such restrictions or regulations shall be considered part of this policy.

V. RESPONSIBILITY

Department Heads and supervisors are responsible for ensuring that all users under their supervision have read this policy and understand its applicability to activities.

Users are responsible for complying with the provisions of this policy and must take full responsibility for their own actions while using the City of Newton's telecommunications systems**.**

VI. PROHIBITED USES

The following uses of the City's telecommunications systems are prohibited:

A. Generally

- Any unauthorized personal use that is not related to City business;
- Any use of the City's telecommunications systems and resources for commercial purposes, private financial gain, political lobbying or unauthorized solicitation or advertising;
- Any use of the City's telecommunications systems for illegal, inappropriate, obscene, defamatory, discriminatory, harassing, threatening or offensive purposes, or in support of such activities;
- Any use of the City's telecommunications systems for purposes in conflict with existing City of Newton policies and procedures;
- Any use of the City's telecommunications systems for the illegal copying, transmission, downloading or installation of copyrighted, trademarked, patented or trade secret materials. These materials include, but are not limited to, writings, articles, web pages, designs, music, videos, photographs and software;

- Any attempt to tamper with, violate, breach or circumvent any security system or device implemented by the City of Newton or other institutions, organizations, companies, or individuals;

- Any knowing vandalism or destruction of computer files or telecommunications equipment; and

- Improper access or misuse of any confidential non-public files, data or information about City of Newton employees or its citizens.

B. Internet & E-mail

- Use of e-mail applications not approved by the IT Department;

- Accessing private e-mail accounts, unless such access is authorized by a user's supervisor or Department Head;

- Falsifying, concealing, or misrepresenting the user's e-mail identity (referred to as "spoofing");

- Anonymous communications;

- Mass e-mailing of unsolicited or unwanted messages ("spamming"), including, but not limited to, text, software, video images, and graphics;

- Using instant messaging, SKYPE, FACEBOOK and similar websites, and texting, unless such access is authorized by a user's supervisor or Department Head;

- Accessing an on-line interactive discussion group or chat room or forum, other than those for which the user has obtained permission from his or her Department Head or supervisor to access;

- Using the City's telecommunications systems to access any information that is pornographic, obscene, sexually explicit or sexually suggestive, profane or vulgar;

- Using the City's telecommunications systems to access or transmit any information that advocates dangerous or illegal acts or that advocates violence or hatred toward any person or group;

- Using the City's telecommunications systems to access or transmit materials that are offensive, threatening or that otherwise are intended to harass or demean recipients, including jokes that are intended to offend, harass or intimidate;

- Downloading digital content of any type, including but not limited to video, music and sound recordings, and image files;

- Streaming video or audio, over the Internet;

- Any personal electronic communication contributing to network congestion; and

- Use of the City's telecommunications systems to communicate in a manner that violates generally accepted rules of e-mail or computer etiquette and/or professional conduct.

C. Computer Network

- Any tampering with computer hardware or software or misuse or disruption of information technology;

- Installation or attempting to install equipment without prior approval by IT such as, but not limited to: wireless access devices, communications equipment, personal information management systems, and the like;

- Unauthorized access, including hacking into or from any City computer;

- Posing as another user, logging on to the system via another user's account, or utilizing the account of another user without permission;

- Knowingly downloading, installing or using programs that infiltrate computing systems and/or damaging software components, including "viruses" and "worms";

- Downloading, installation and use of any program or software without prior authorization by IT;

- Intentionally disrupting network traffic, crashing the network, or gaining unauthorized access to the files of another user;

- Using inappropriate language in any type of communication on the City's network. Inappropriate language includes, but is not limited to, language that is vulgar, profane, abusive or threatening;

- Using the City's network to personally attack, harass, or threaten another person or intentionally or recklessly publishing false information about another person; and

- Playing computer games, unless part of an educational or training program that has been approved by IT.

VII. NETWORK ACCOUNTS AND PASSWORDS

Each authorized user will be provided with one or more network accounts. Each user must use a password to access the account. Users are personally responsible at all times for the proper use of those accounts.

Leaving personal account information, including passwords on, in, or around any City computer is prohibited.

Unauthorized sharing of any network accounts and/or passwords with anyone is prohibited.

In order to avoid unauthorized access to user accounts, it is advisable that user connections to any networked resource not be left open and unattended. Subject to department head discretion, this guideline can be made mandatory within a department.

VIII. REMOTE AND VIRTUAL PRIVATE NETWORK (VPN) ACCESS

A VPN is a virtual private network, which is a remote, off-site connection to the City's Wide Area Network (WAN) from any non-City location. City employees provided with remote access by IT shall be the exclusive users of the City's network from the remote, non-City location. They are prohibited from sharing their password with anyone else, and shall be responsible for any harm resulting from inappropriate sharing of the password. Any remote access to the City's network, including high-speed connections (e.g., cable modems, DSL, analog or wireless), is prohibited unless approved by IT.
Remote access directly to any City office's Local Area Network (LAN), or stand-alone personal computer (PC) using any remote access software, without permission from IT, is prohibited.

It is the responsibility of the VPN user to ensure that unauthorized access to the City's network via the user's VPN access does not occur.

It is the responsibility of the VPN user to ensure their personal computer is up to date with antivirus and operating system patches.

It is the responsibility of the VPN user to ensure that any components attaching to the City network are secure.

By using VPN access through a personal computer (desktop, laptop, cellular phone or similar device), users agree that they are subject to the same rules and regulations that apply to City-owned equipment.

VPN access is only granted after approval from IT. The City will conduct audits periodically to detect the presence of software that allows remote access. Anyone with unauthorized VPN software installed on City equipment will be in violation of this policy.

The IT Department retains the right to terminate a VPN connection on either a short term basis or permanently if harm to the LAN, WAN or City equipment is deemed to originate from a VPN user's connection. Violations of this policy may result in removal of a user's VPN access and discipline, up to and including termination from employment.

IX. TELEPHONE RULES

In the event that there is an additional charge incurred for an employee's personal use of the City's telephone service, both land line and cellular, the user will reimburse the City.

City cellular phones should not be used while engaging in hazardous activities requiring focused attention.

X. REPORTING ALLEGED POLICY VIOLATIONS

Violations of this policy must be reported by an employee to his/her supervisor, Department Head, the Director of Human Resources or the Executive Office.

XI. NO EXPECTATION OF PRIVACY

Any and all information contained in computers (desktop, laptop, cellular phone or similar devices), computer files, e-mail messages, or voice mail messages is the property of the City. As such, the City may access any information contained therein at any time.

Users should have no expectation of privacy in their use of the City's telecommunications systems.

Users should be aware that computer files, e-mail, texts, and voice mail messages may constitute public records under G.L. c. 4, § 7 (26), and may be subject to disclosure under G.L. c. 66, § 10. This includes, but is not limited to, computer files, e-mail messages and voicemail originating from personal accounts that are used for the conduct of City business.

XII. MONITORING OF TELECOMMUNICATIONS SYSTEMS

Upon the request of the Department Head and/or the Director of Human Resources, and subject to the approval of the Mayor, monitoring of any and all telecommunications systems usage may be necessary. Reasons for monitoring include, but are not limited to, review of employee productivity, investigations into claims of possible criminal activity,

and investigations into violations of this policy. Use of the City's telecommunications systems by any user constitutes consent to monitoring of systems use and is conditioned upon strict adherence to this policy.

Any City employee assigned to perform this monitoring shall receive the cooperation of all other City employees in carrying out this task. Any City employee failing to provide such cooperation or interfering with his/her effort to perform said monitoring tasks, may be subject to discipline, up to and including termination from employment. Any violations of this policy discovered either as a result of this monitoring or as an incident to the normal course of routine work will be reported to the Executive Office, the Director of Human Resources and to the appropriate Department Head.

Policy Adopted: January 13, 2012

APPENDIX A

Definitions

Components - Components are any internal parts of a computer.

Computer Viruses – In this document, computer virus is a catchall phrase that refers to applications such as self-replicating software, adware, spyware, computer worms, Trojan horses, rootkits and malware. The specifics of each vary, but the common denominator is that they should be preventable using updated protection and avoiding questionable websites and unauthorized files.

Hacking - Computer hacking is broadly defined as knowingly accessing a computer without authorization or exceeding authorized access. Various state and federal laws govern computer hacking.

Hardware - Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM (Random Access Memory).

Illegal Use - Any violation of local, state, or federal laws or regulations.

LAN - A LAN (Local Area Network) supplies networking capability to a group of computers in close proximity to each other such as in an office building, a school, or a home.

Network - A computer network is a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information.

Network Broadcast Messages - A message that is sent to all users of a computer network when they log on to the network.

Network Congestion – When data requests exceed the available bandwidth to supply all user needs, network traffic begins to slow down

Patches – Patches are software repairs intended to close a flaw in code originally released by the developer. Patches attempt to reduce the potential for hackers to obtain access to a PC through mistakes in code.

Security – The ability of a system to protect information and system resources with respect to confidentiality and integrity.

Software - Computer software is a general term that describes computer programs. Related terms such as software programs, applications, scripts, and instruction sets all fall under the category of computer software. Software is code written by computer programmers that is compiled into a computer program.

WAN - A WAN (Wide Area Network) supplies networking capability to a group of computers across metropolitan, regional, or national boundaries.